Dell Data Protection | Encryption

Using CertAgent to Obtain Domain Controller and Smart Card Logon Certificates for Active Directory Authentication

© 2014 Dell Inc.

Registered trademarks and trademarks used in the DDP|E, DDP|ST, and DDP|CE suite of documents: Dell™ and the Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, and KACE™ are trademarks of Dell Inc. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, and Xeon® are registered trademarks of Intel Corporation in the U.S. and other countries. Adobe®, Acrobat®, and Flash® are registered trademarks of Adobe Systems Incorporated. Authen Tec® and Eikon® are registered trademarks of Authen Tec. AMD® is a registered trademark of Advanced Micro Devices, Inc. Microsoft®, Windows®, and Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, Skydrive®, SQL Server®, and Visual C++® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. VMware® is a registered trademark or trademark of VMware, Inc. in the United States or other countries. Box® is a registered trademark of Box. Dropbox℠ is a service mark of Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube®, and Google™ Play are either trademarks or registered trademarks of Google Inc. in the United States and other countries. Apple®, Aperture®, App Store℠, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®℠, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari®, and Siri® are either servicemarks, trademarks, or registered trademarks of Apple, Inc. in the United States and/or other countries. GO ID®, RSA®, and SecurID® are registered trademarks of EMC Corporation. EnCase™ and Guidance Software® are either trademarks or registered trademarks of Guidance Software. Entrust® is a registered trademark of Entrust®, Inc. in the United States and other countries. InstallShield® is a registered trademark of Flexera Software in the United States, China, European Community, Hong Kong, Japan, Taiwan, and United Kingdom. Micron® and RealSSD® are registered trademarks of Micron Technology, Inc. in the United States and other countries. Mozilla® Firefox® is a registered trademark of Mozilla Foundation in the United States and/or other countries. iOS® is a trademark or registered trademark of Cisco Systems, Inc. in the United States and certain other countries and is used under license. Oracle® and Java® are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. SAMSUNG™ is a trademark of SAMSUNG in the United States or other countries. Seagate® is a registered trademark of Seagate Technology LLC in the United States and/or other countries. Travelstar® is a registered trademark of HGST, Inc. in the United States and other countries. UNIX® is a registered trademark of The Open Group. VALIDITY™ is a trademark of Validity Sensors, Inc. in the United States and other countries. VeriSign® and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. KVM on IP® is a registered trademark of Video Products. Yahoo!® is a registered trademark of Yahoo! Inc.

This product uses parts of the 7-Zip program. The source code can be found at www.7-zip.org. Licensing is under the GNU LGPL license + unRAR restrictions (www.7-zip.org/license.txt).

2014-02

Protected by one or more U.S. Patents, including: Number 7665125; Number 7437752; and Number 7665118.

Information in this document is subject to change without notice.

Contents

Domain Controller Certificates 5

Enrollment for a Domain Controller Certificate **5**

Issuing a Domain Controller Certificate **5**

Installing the Domain Controller Certificate **6**

Smart Card Logon Certificates 7

Enrollment for a Smart Card Logon Certificate **7**

Issuing a Smart Card Logon Certificate **7**

Installing a Smart Card Logon Certificate **7**

Domain Controller Certificates

Enrollment for a Domain Controller Certificate

To initiate the process of obtaining a suitable certificate, a system administrator on the domain controller system should do the following:

1. Generate an "offline" domain controller certificate request following the instructions on the Microsoft Technet website:
   http://technet.microsoft.com/en-us/library/cc783835%28WS.10%29.aspx
2. Open a browser and go to the **Upload Certificate Request** page of the CertAgent public site and submit the request file (typically named <dcname>-req) to an appropriate CA.
3. Once your request has been accepted, make a note of the **request ID** generated by the CertAgent system to aid in the certificate retrieval process (described below).

Issuing a Domain Controller Certificate

The CertAgent CA to whose account the request has been submitted should follow these steps in issuing the domain controller certificate:

1. Login to the appropriate CertAgent CA account; this is the account that you will be using to issue the domain controller certificate.
2. Open the pending certificate request list and click the request you wish to process. This will open the advanced options dialog.
3. If you already know the globally unique identifier (GUID) of the domain controller for which the certificate will be issued, skip to the next step. Otherwise, you can determine the required GUID as follows:
   - click **Export** and *save the certificate request to a file*
   - open a Command Prompt and run the following command:

     `certutil -dump <request file>`
   - the required domain controller GUID may be found in the output of this command as the value associated with the OID 1.3.6.1.4.1.311.25.1 as shown below:

```
Subject Alternative Name
   Other Name:
        1.3.6.1.4.1.311.25.1= 0410 6661 6135 3636 3234 3831 6263 3866 6662
```

   - copy the entire domain controller GUID to the clipboard and return to CertAgent
4. Select **Issue certificate with customized settings** from the *Action* drop-down list.
5. Customize the included extensions as described here (if they are not already specified in the active CA's default certificate profile settings):
   - under CRL Distribution Point, enter a valid CRL distribution point URL.

- under Key Usage, make sure that only the **digital signature** and **key encipherment** checkboxes are checked.
- under Extended Key Usage, check only the following checkboxes: **client authentication**, **server authentication**, and **MS: Smart Card Logon**.
- under Subject Alternative Name, add an **Other Name** field and complete its attributes as follows:

  specify an **OID** of **1.3.6.1.4.1.311.25.1**

  set **Octet String** as the type of this attribute and enter the domain controller's GUID as its value; then carefully remove the first four characters (**04??**) and all spaces and insert **0x** at the front of the string (to ensure it is interpreted in hex).

  For example, if the GUID was originally **0410 6661 6135 3636 3234 3831 6263 3866 6662** as above, you would enter **0x66613536363234383162633866666662** as the hexadecimal value of the new attribute.
- under Subject Alternative Name, add a **DNS Name** and specify the DNS name of the domain controller.
- enter the following base64-encoded data as a Custom Extension:

```
MC8GCSsGAQQBgjcUAgQiHiAARABvAG0AYQBpAG4AQwBvAG4AdAByAG8AbABsAGUAcg==
```

NOTE: When you copy and paste this value, be sure to capture the two trailing equal signs. This extension is required to ensure that the certificate is accepted and processed as a domain controller certificate by the default policy module in the domain controller.

- Basic Constraints are optional, but if you include them be sure to deselect the *CA* checkbox.

6 Review the changes and then click **Submit** to issue the certificate.

If you are doing this often, you should configure a CA account or sub-account to include the custom extensions automatically so that only minor editing of attribute values is required on a per-request basis. For a detailed discussion of the constraints on the contents of a Microsoft domain controller certificate, see http://support.microsoft.com/kb/291010.

Installing the Domain Controller Certificate

Once the domain controller certificate has been issued, the system administrator may install it by following these steps:

1 Go to the **Retrieve Certificate** page of the CertAgent public site.

2 Enter the **request ID** and click **Retrieve**.

3 Click the link labeled **Download this certificate path to a local base64-encoded PKCS#7 file** and save the PKCS#7 file to a convenient folder on your computer.

4 Install the domain controller certificate by running the following command at a Command Prompt:

```
certreq -accept <PKCS#7 filename>.
```

For a more detailed discussion of the installation process for a domain controller certificate, see http://technet.microsoft.com/en?us/library/cc785678%28WS.10%29.aspx.

Smart Card Logon Certificates

Enrollment for a Smart Card Logon Certificate

Any entity wishing to obtain a smart card logon certificate for use with Active Directory can initiate the process by following these steps:

1. Go to the **Enroll Certificate using Browser** page for an appropriate CA account/sub-account on the public side of the CertAgent website.
2. Select the **CSP** associated with your smart card.
3. Select **Both** for the **Key Usage** value.
4. Deselect the checkbox labeled **Mark keys as exportable**.
5. Fill in the rest of the form and click **Submit**.
6. Once your certificate request has been accepted, make a note of the request ID generated by the system.

Issuing a Smart Card Logon Certificate

A CertAgent CA may follow these steps to issue the certificate:

1. Login to the CertAgent CA account to which the certificate request has been submitted.
2. Click the desired certificate request from the pending list to open the advanced dialog.
3. Select **Issue certificate with customized settings** from the *Action* drop-down list.
4. Customize the extensions for this certificate as follows:
   - under CRL Distribution Point, enter a CRL distribution point URL.
   - under Key Usage, check only the **digital signature** checkbox.
   - under Extended Key Usage, check only the **client authentication** and **MS: Smart Card Logon** checkboxes.
   - under Subject Alternative Name, add an **Other Name** field and complete its attributes as follows:

     specify an **OID** of **1.3.6.1.4.1.311.20.2.3**

     set **UTF8 String** as the type of the attribute and enter the principal name as its value (for example, user1@dell.com).
   - Basic Constraints are optional, but if you include them be sure to deselect the *CA* checkbox.
5. Review the changes and then click **Submit** to issue the certificate.

For more detailed instructions on enabling smart card logon, see http://support.microsoft.com/kb/281245.

Installing a Smart Card Logon Certificate

Once a smart card logon certificate has been issued, the entity who requested it may retrieve it and install it on their computer as follows:

1. Go to the **Retrieve Certificate** page of the CertAgent public site.

2 Enter the **request ID** for your certificate and click **Retrieve**.

3 Click the link labeled **Install this certificate path into CAPI/CNG** and follow the prompts to install your certificate.

0 XXXXXA0 X